

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

**ІТ-ПРАВО
ПІД ЧАС ГІБРИДНОЇ ВІЙНИ:
ВІД ПОШУКУ ПАРАДИГМИ
ДО ПРАГМАТИЧНИХ РІШЕНЬ**

Колективна монографія

*За редакцією
Є. Харитонова, О. Харитонової, І. Давидової*

Одеса
Фенікс
2025

*Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)*

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

I-87 **ІТ-право під час гібридної війни: від пошуку парадигми до практичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ЗМІСТ

Авторський колектив	5
Розділ 1. Прагматична (соціологічна) школа «ІТ-права» – відповідь цивілістики на виклики інформаційного суспільства (Євген Харитонов, Олена Харитонova, Ірина Давидова)	7
Розділ 2. Концепт ІТ-права (Євген Харитонов, Олена Харитонova)	30
Розділ 3. Гібридна інформаційна війна та інформаційні технології (Євген Харитонов, Олена Харитонova)	65
Розділ 4. ШІ як бінарна категорія ІТ (Євген Харитонов, Олена Харитонova)	93
Розділ 5. Симулякр, гібридна (інформаційна) війна і потенціал ІТ (Євген Харитонов, Олена Харитонova)	119
Розділ 6. Інформаційне середовище як стратегічний ресурс у гібридних конфліктах (Оксана Калітенко)	143
Розділ 7. Правові рамки для цифрових активів: перспективи цифрової власності (Катерина Некіт)	175
Розділ 8. Захист немайнових прав у медіапросторі в період гібридної війни (Алла Кирилюк, Лариса Галупова)	203
Розділ 9. ІТ-правочини в умовах гібридної війни (Ірина Давидова)	250
Розділ 10. Порушення прав інтелектуальної власності в мережі інтернет під час гібридної агресії в умовах воєнного стану (Наталія Бааджи)	279
Розділ 11. Кіберзагрози у гібридній кібервійні: дія і протидія (Євген Харитонов, Олена Харитонova)	323
Розділ 12. Етико-юридичні аспекти використання штучного інтелекту в мережі інтернет в умовах гібридної війни (Олександр Омельчук)	351
Розділ 13. Застосування систем автоматизованого прийняття рішень під час збройного конфлікту (Віра Токарева)	378

Розділ 14. Гібридна війна і кіберзброя (Євген Харитонов, Олена Харитонova)	388
Розділ 15. Вербування неповнолітніх через соцмережі та месенджери в умовах гібридної війни: загрози, механізми та заходи запобігання (Вікторія Рябченко).	420
Розділ 16. Правове регулювання діяльності стартапів в умовах гібридної війни: виклики, можливості та перспективи (Дмитро Розумейко).	435
Розділ 17. Е-кредитування у період воєнного стану (Олена Берназ-Лукавецька)	453
Розділ 18. Цивільно-правова відповідальність за шкоду, завдану кібератаками (Богдан Фасій)	483
Розділ 19. Сімейні правовідносини в сфері інформаційних технологій в умовах гібридної війни (Оксана Сафончик)	514
Розділ 20. Забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні (Крістіна Дрогозюк)	545
Розділ 21. Кіберспортивна дипломатія: перспективи для України (Максим Ткалич, Юлія Толмачевська)	557
Список основних праць представників школи	565

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонova Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561), кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031), аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492), аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 13

ЗАСТОСУВАННЯ СИСТЕМ АВТОМАТИЗОВАНОГО ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

DOI

Віра Токарева

кандидатка юридичних наук, доцентка

По мірі впливу четвертої промислової революції на сучасне життя, зростає значення технологій великих даних та машинного навчання у суспільстві. Аналіз великих даних та предикативної аналітики дозволяє передбачувати ймовірні майбутні події, поведінку контрагентів, розраховувати ризики та допомагає приймати рішення¹. Системи автоматизованого прийняття рішень покликані покращити процес вибору та прийняття рішень. Попри те, що технології машинного навчання та автоматизованого прийняття рішень наразі, вони вже використовуються у медицині для виявлення осіб та ризиків розвитку патологій, для проведення профілактичного лікування², у судочинстві для профілювання, оцінки ризиків та прогнозування ймовірності повторного вчинення правопорушень³, у фінансовій сфері при прийнятті рішень про видачу кредиту, визначення платоспроможності, тощо. Технології машинного навчання, аналізу великих даних, дистанційної біометричної ідентифікації, зокрема, використовуються під час аналізу розвідувальних даних та збройних конфліктах.

Під час збройних конфліктів особливу роль відіграють системи підтримки прийняття рішень на основі ШІ, які аналізують дані та розробляють рекомендації для прийняття рішень. У порівнянні із повністю автономними системами озброєння, перевагами систем під-

¹ Rainie L., Anderson J. Code-dependent: pros and cons of the algorithm age. 2017. № 8. Р. 2-41. 02/08181534/PI_2017.02.08_Algorithms_FINAL.pdf

² Faggella D. Applications of Machine Learning in Pharma and Medicine. *Tech Emergence*. July 19, 2018. URL: <https://www.techemergence.com/machine-learning-in-pharma-medicine/>

³ Токарева В. О. До питання прийняття рішень із застосування алгоритмів. *Публічне та приватне право*. 2023. № 1. С. 30-35. URL: http://pp-law.in.ua/archive/1_2023/5.pdf

тримки прийняття рішень на основі ШІ є допомога в прийнятті оптимальних рішень особі та підвищення обізнаності про ситуацію ¹.

Поряд із значною увагою, дослідженню правових питань застосування технологій обробки великих даних, автоматизованих систем прийняття рішень, машинного навчання, віддаленої біометричної ідентифікації, застосування даних технологій в умовах збройного конфлікту, заслуговує пильної уваги. Застосування вищезгаданих технологій у збройному конфлікті актуалізує наступні питання.

По-перше, використання машинного навчання, може призвести до автоматизації окремих видів самооборони. Насьогодні, використовуються подекуди, автоматизовані системи реагування, які є стаціонарними оборонними системами, призначеними лише для реагування на вхідні загрози і мінімізації шкоди.

По-друге, поширення використання автоматизованих систем для допомоги прийняття рішень людиною актуалізує питання достовірності та надійності результатів такого аналізу, а також ступеня довіри людиною рекомендаціям алгоритмів. Актуалізується питання, здатності людини відкинути вочевидь хибне рішення запропоноване алгоритмом та прийняти рішення опираючись на власні переконання, досвід та судження.

По-третє, дискусії щодо використання технологій машинного навчання актуалізують питання прозорості процесу прийняття рішень, через нерозуміння логіки функціонування алгоритмів. Порід із цим, непрозорість рішень або рекомендацій автоматизованої системи, обумовлено тим, що її функціонування захищено як об'єкт права інтелектуальної власності ².

Висуваються позиції, що використання систем прийняття рішень на основі ШІ може допомогти ефективно захищати цивільне населення під час збройного конфлікту. Оскільки система швидко сканує та аналізує ситуацію³. Разом з тим, дане твердження залишається вель-

¹ Zhou W. Greipl A. R. Artificial Intelligence in military decision-making: supporting humans, not replacing them August 29, 2024. URL: <https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/>

² Zwanenburg M. Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law. *International Law Studies (Naval War College)*. 2021. № 97. P. 1404-1431.

³ Joint Statement on Lethal Autonomous Weapons Systems First Committee, 77th United Nations General Assembly Thematic Debate – Conventional Weapons URL: https://estatements.unmeetings.org/estatements/11.0010/20221021/A1jJ8bNfWGIL/KLw9WYcSnnAm_en.pdf

ми дискусійним. Безумовно, міжнародне гуманітарне право зобов'язує військових командирів та інших осіб, відповідальних за напади, засновувати свої рішення на інформації з усіх джерел, доступних їм у відповідний момент часу. Зокрема, Міжнародний Комітет Червоного Хреста (далі МКЧХ) в контексті ведення міської війни рекомендує, проводити перевірку даних про наявність цивільних осіб та цивільних об'єктів, у відкритих джерелах, таких як Інтернет. Відповідно до висновків МКЧХ системи підтримки прийняття рішень на основі ШІ можуть допомагати збору, обробці даних з метою оперативного прийняття рішень та мінімізації ризиків для цивільного населення ¹.

Водночас, будь-яка інформація, отримана за допомогою автоматизованих систем, має бути перевірена з різних джерел, щоб уникнути упередженої або неточної інформації. Проте, МКЧХ констатує складність проведення такої перевірки, а іноді й неможливість, через специфіку функціонування системи та способу взаємодії людини з автономними машинами.

Крім того, відповідно до міжнародного гуманітарного права, сторони збройного конфлікту, а саме людина, а не алгоритм несе відповідальність за дотримання норм права. Тому, дотримання норм міжнародного гуманітарного права покладається виключно на уповноважених осіб. Разом з тим, командувачі відповідальні за прийняття рішення та здійснення атак, можуть використовувати технологічну підтримку на підставі систем ШІ, для обґрунтування прийнятих власних рішень. Наразі, розроблені системи дозволяють проводити ідентифікацію осіб та об'єктів, оцінювати озброєння супротивника та нанесенні збитки. Відтак, при виборі цілі для атаки, можуть використовуватися системи підтримки прийняття рішень на основі ШІ, рішення яких носять рекомендаційний характер. Рекомендації таких систем не заміщають людину при прийнятті остаточного рішення ².

Перевагою використання автоматизованих систем, також називають зменшення часу для прийняття рішення, даючи таким чином стороні переваги у порівнянні з його супротивником.

Оскільки алгоритми машинного навчання, створені для передбачення майбутніх подій, держави прагнуть створити «системи ранньо-

¹ Stewart R. Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. October 24, 2023. URL: <https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/>

² Там само.

го попередження», які б дозволяли виявляти майбутні загрози. Наразі, алгоритми дозволяють встановлювати місця розташування, переміщення озброєння. Навіть, виявляти посилення частоти листування на тему атак та загроз. Алгоритми здатні аналізувати та рекомендувати розташування представників правоохоронних органів у місцях, де існує висока вірогідність вчинення правопорушень. Алгоритми машинного навчання дозволяють виявляти зміни у висвітленні новин в авторитарних режимах напередодні збройного конфлікту. Такі інструменти можуть надавати критично важливу інформацію державам, у разі високої вірогідності збройного нападу сусіда. Безумовно, така аналітика та оцінка ризиків на основі машинного навчання має оцінюватися всебічно та приймати до уваги потенційні упередження¹.

Відносно використання системи дистанційної біометричної ідентифікації під час збройного конфлікту, то такі системи покликані забезпечити точне застосування озброєння під час конфлікту, ніж, наразі, відбувається. Якщо від початку технології біометричної ідентифікації, як такі, розроблялися для цивільного застосування, зі спливом часу стали використовуватися під час збройних конфліктів. Наразі, збройні сили США мають найбільший досвід впровадження біометричної ідентифікації під час ведення військових операцій².

Технології біометричної ідентифікації можуть використовуватися в усьому спектрі операцій ведення збройного конфлікту: веденню бойових дій, забезпеченню безпеки, підтримання миру та військовими діями в мирний період. Технологія біометричної ідентифікації дає змогу з високим ступенем достовірності конкретно ідентифікувати особу та ворожу загрозу.

Використання технологій біометричної ідентифікації застосовується Організацією Північноатлантичного договору (НАТО) для розпізнавання суб'єктів які несуть загрози. У 2020 році НАТО оголосила про створення власної Автоматизованої системи біометричної ідентифікації, розробленої Агентством зв'язку та інформації НАТО³.

¹ Deeks A., Lubell N., Murray D., Machine Learning, Artificial Intelligence, and the Use of Force by States. *Journal of National Security Law & Policy*. 2019. № 10. URL: <https://ssrn.com/abstract=3285879>

² Mitchell A. Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics. *Canadian Yearbook of International Law*. 2012. № 50. P.289-297.

³ Див.: Zwanenburg M. Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law.

Серед аргументів проти використання автоматизованих систем та біометричної ідентифікації, зокрема, під час збройного конфлікту, слід назвати, упередження, помилки у ідентифікації алгоритмів, брак прозорості тощо.

Відносно такої переваги як зменшення часу для прийняття рішення, слід зазначити, що стратегія та тактика військового планування передбачає необхідність прийняття рішень військовим командуванням з урахуванням аналізу оперативної обстановки, місцерозташування супротивника та цивільного населення, оцінки переваг та недоліків вірогідних варіантів подій. У свою чергу, використання автоматизованих систем, в наслідок скорочення часу для ухвалення рішення, знижує здатність людини об'єктивно оцінити ситуацію. У випадку використання систем підтримки прийняття рішень на основі ІІІ людина отримує обмежену інформацію про логіку «рекомендованого» рішення ІІІ та аргументів які лягли в основу такої рекомендації. До того, ж як свідчать спостереження, використання автоматизованих систем здатне знизити пильність та здатність людини зберігати об'єктивну оцінку ситуації.

Серед помилок, слід назвати, некоректне розпізнавання осіб через ознаки шкіри, рекомендація маршрути руху транспорту без врахування актуальних дорожніх умов, некоректне розпізнавання стін та відбійників, що приводило до ДТП за участі автономних транспортних засобів, тощо. Відтак, автоматизована система може бути введена в оману. Наприклад, під час конфлікту, через некоректне функціонування алгоритму, під час наведення на ціль цивільний транспортний засіб може бути ідентифікований як ворожий та навпаки ¹.

По мірі зростання використання автоматизованих систем для розв'язання дедалі складніших завдань, накопичення досвіду навчання та прийняття рішень, стає складнішим перевірка помилок, які сприяли отриманню кінцевого результату. В свою чергу по мірі ускладнення систем, зростає ймовірність вчинення помилок, адже, навіть, невелика неточність у навчальних даних та розробці систем, може призвести до повторення помилок та виведення їх у еталоне значення.

¹ Див.: Deeks A., Lubell N., Murray D., Machine Learning, Artificial Intelligence, and the Use of Force by States.

Прийнято виділяти такі основні види упереджень: 1) упередження у навчальних даних; 2) упередження у дизайні та розробці; 3) упередження у використанні програми. Це означає, що упередження можуть виникати протягом усього життєвого циклу алгоритмічних моделей, починаючи зі збору даних, навчання, використанні тощо ¹.

Упередженості у навчальних даних обумовлені тим, що будь-які навчальні дані відображають певну обмежену вибірку. Така вибірка може містити як прямі упередження, щодо стереотипу, так і непрямі упередження щодо частоти їх виникнення. Відтак, упередженості у даних виникають внаслідок не репрезентативності даних або неповноти представлених даних, що призводить до нерепрезентативних результатів. Таким чином, упередження виникають, коли певні типи даних відсутні або представлені більше, ніж інші, що часто пов'язано зі способами отримання даних. Відтак, якість вхідних навчальних даних, визначає якість результату який буде отриманий. Оскільки система ІІІ навчається відповідно до скормлених їй навчальних даних, які є єдиною інформацією яка використовується на етапі навчання та тестування, то неточності у цих даних, у подальшому будуть у підсумкових рішеннях.

Упередженості у дизайні та розробці. Упередженість даних може посилюватися на різних етапах обробки даних, наприклад, під час навчання моделі. Під час процесу навчання моделі штучного інтелекту, програмісти та інженери роблять проводять анотування, маркування, класифікація зразків даних, моделювання, оцінку моделі тощо. Таким чином, алгоритмічні упередження можуть також бути результатом, несвідомих упереджень, які люди вносять у життєвий цикл системи машинного навчання через різні завдання, які вони виконують. Поряд із цим упередження можуть виникати через відсутність прозорості функціонуванням алгоритму. На цьому етапі технології ІІІ відображають упередження, притаманні навчальним даним та упередженням розробників.

Упередженості обґрунтовані використанням автоматизованих систем. Технології ІІІ, як такі, будуть нести упередження через їх поширення та по мірі їх використання. Будь-які упередження, які

¹ Bode I. Falling under the radar: the problem of algorithmic bias and military applications of AI. March 14, 2024. URL: <https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/>

містить система ШІ, будуть посилюватися, вводючи їх в еталон. В тому числі, через те, що люди схильні надмірно покладатися на результати які пропонує їм система, навіть, попри їх очевидну хибність. Таким чином існує вірогідність, що системи будуть генерувати все «більше даних заснованих на вже упереджених рішеннях». Таким чином, упереджені результати, отримані за допомогою технологій ШІ, також можуть бути додатковим виправданням для існуючих упереджень. На етапі використання технологій необхідно приймати до уваги упередженості у тому, як люди взаємодіють з технологіями ШІ, насамперед упередженість автоматизації. Наразі існує тенденція, що людина надмірно покладається на рекомендації автоматизованих систем та надмірно довіряє результатам, отриманим за допомогою таких технологій¹. Існує чимало доказів упередженості щодо автоматизації, отриманих з досліджень поза межами військової сфери. Тому, на жаль, ми можемо легко уявити собі ситуації, коли люди занадто довіряють системам штучного інтелекту у військовому контексті.

Так, наприклад, у період поширення коронавірусної інфекції, відомі випадки, коли система розпізнавання обличчя встановлена на об'єктах транспортної структури в одному із мегаполісів світу, розпізнала людину як таку, що перебуває у розшуку, при цьому черговим співробітниками поліції, було очевидно, що людина яку вони затримують, не схожа на особу яка перебуває в розшуку, але автоматизована система його розпізнала. Упередження автоматизації виявилось у тому, що співробітники поліції, навіть, розуміючи абсурдність затримання, віддали перевагу рішенням алгоритму, а ніж власними очам, уявленням про справедливість та законність.

Наслідком упереджень, невідомості як працює система «чорного ящика», є спроби підігнати та обґрунтувати рішення алгоритму. Американським фахівцями пропонується називати – алгоритмічним або математичним відмиванням (переклад з «mathwashing» або «farewashing») випадки коли суб'єкт намагається підвести будь-яку логіку та обґрунтувати рішення алгоритму, знайти правдоподібне логічне пояснення рішенням алгоритму, яке не має розумних підстав

¹ Proceed with Caution: Artificial Intelligence in Weapon Systems. Ordered to be printed 23 November 2023 and published 1 December 2023. Report of Session 2023–24. Published by the Authority of the House of Lords. URL: <https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/16.pdf>

обґрунтування. Іншими словами алгоритмічне або математичне відмивання відбувається коли суб'єкт перестає довіряти собі, а автоматично обирає довіряти програмі, нехтуючи критичним мисленням. Ф. Бененсон, колишній начальник відділу даних Kickstarter зазначив, що математичне відмивання виникає внаслідок надмірної ідеалізації діяльності алгоритмів¹. Т. Шеп відрізняє математичне відмивання яке відбувається випадково та яке проводиться цілеспрямовано. Відмивання відбувається випадково (суб'єкт обґрунтовує правдоподібність рішення алгоритму не навмисно, не розуміє вразливість рішення алгоритмічної системи) або цілеспрямовано (коли суб'єкт дотримуються, очевидно упередженого рішення прийнятого системою). Цілеспрямоване дотримання, вочевидь, упередженого рішення може бути обумовлено тим, що особа побоюється публічного осудження, бажає зберегти репутацію, хоча для суспільства є очевидним упередженість рішення алгоритму². Проблема постає із розумінням упередженості як такої, оскільки стандарту упередженості не існує і також варіюється залежно від історичних, територіальних чинників, соціальних груп, релігійної приналежності, статі, тощо. Так, наприклад, 100 років тому не визнавалося упередженістю недопущення жінок до певних професій та посад. Водночас, сьогодні встановлення будь-яких обмежень, щодо зайняття жінками певних посад або певної діяльності буде визнано упередженістю. Прикладом упередженості для більшості цивілізованих держав світу, також є різний обсяг прав осіб в залежності від віросповідання. Тому, провідною умовою успішного функціонування алгоритмів, під час розробки та роботи є недопущення різного ставлення та різного обсягу прав суб'єктам, соціальним групам.

Відтак, можна припустити, що упередження у системі можуть призвести до неминучих наслідків, якщо суб'єкт певного віку, статі, расової приналежності буде помилково ідентифікований системою в якості комбатанта³. Упередження крім того впливають на функціональність і передбачуваність систем. Рішення можуть залишатися не

¹ Byrnes N. Why We Should Expect Algorithms to Be Biased 2016. URL: <https://www.technologyreview.com/2016/06/24/159118/why-we-should-expect-algorithms-to-be-biased/>

² What is mathwashing? url: <https://www.mathwashing.com>

³ Chandler K. Does military AI have gender? Understanding bias and promoting ethical approaches in military applications of AI. UNIDIR, Geneva, 2021. URL: <https://doi.org/10.37559/GEN/2021/04>

ясними та незрозумілими, через брак інформації яким саме властивостям алгоритм надав переваги. Відтак, упередженість у навчальних даних, що використовуються для цивільного та військового застосування може посилюватися. Причиною може бути, використання навчальних даних які не приймають до уваги специфіку збройного конфлікту, коли дані відображають конкретний конфлікт або операцію, які не можуть бути застосовані у іншому випадку.

Вирішення проблеми алгоритмічної упередженості вимагає докорінної зміни дискримінаційного ставлення. Наприклад, на етапі розробки системи мають бути інтегровані стратегії пом'якшення наслідків.

Значної уваги потребує прийняття рішення про застосування сили, під час встановлення об'єкту нападу. Досить широкий спектр завдань і рішень, до яких може застосовуватися ІІІ, також може нести наслідки для осіб які постраждали внаслідок збройного конфлікту, наприклад, у разі застосування арешту, затримання тощо.

МКЧХ наголошує про необхідність збереження контролю людини за рішеннями які можуть нести ризики та вплив для життя та здоров'я в умовах збройного конфлікту. Системи ІІІ мають використовуватися саме в якості інструментів, здатних допомогти в прийнятті рішень людиною, але в жодному разі не замінити її. З огляду на те, що системи ІІІ розробляються для виконання завдань, які зазвичай виконуються людиною, залишається суперечність між прагненням до застосування ІІІ та центральною роллю людини в збройному конфлікті, яка потребує подальшого дослідження. МКЧХ наголошує, на важливості забезпечення людиноцентричного підходу при розробці та використанні ІІІ ¹.

Підсумовуючи вищевикладене, з урахуванням низької прозорості функціонування автоматизованих систем, упередженості, прийняття юридично значущих має здійснювати виключно людина. Особливого значення набуває залишення контролю та ухвалення остаточного рішення за людиною у разі завдання шкоди здоров'ю та життю людям, пошкодження, руйнування цивільної інфраструктури, покладення відповідальності та дотримання сумлінності використання новітніх

¹ ICRC and International Federation of Red Cross and Red Crescent Societies, The Fundamental Principles of the International Red Cross and Red Crescent Movement: Ethics and Tools for Humanitarian Action, Geneva, November 2015. URL: <https://shop.icrc.org/les-principes-fondamentaux-de-la-croix-rouge-et-du-croissant-rouge-2757.html>.

технологій та недопущення зловживання правом у збройних конфліктах. Оскільки, не можна допустити ситуацію, при якій рішення про позбавлення людини життя, буде приймати алгоритм.

Ключові слова: штучний інтелект, біометрична ідентифікація, автоматизовані системи прийняття рішення, міжнародне гуманітарне право, машинне навчання, ІТ-право, інформаційні технології, інформаційне суспільство, цифрова доба, гібридна війна, воєнний стан.